PATENT **Docket No. 356952.00052**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

INVENTORS:	**Craig Heath and Leon Clarke**	Confirmation No. **1329**
APPLICATION NO.	**10/596,774**	
FILED:	**May 25, 2007**	Examiner: **B. Squires**
CASE NO.	**356952.00052**	Group Art Unit: **2431**

TITLE: **A METHOD FOR SECURE OPERATION OF A COMPUTING DEVICE**

FILED ELECTRONICALLY ON January 20, 2010

Commissioner for Patents
MAIL STOP APPEAL BRIEF-PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

Attention: Board of Patent Appeals and Interferences

APPELLANTS' BRIEF

This brief is in furtherance of the Notice of Appeal filed in this case on November 20, 2009. The Commissioner is authorized to charge the fee for filing of this Appeal Brief to Deposit Account No. 50-4364.

1. REAL PARTY IN INTEREST

The present application is assigned to Nokia Corporation, having its principal place of business at Keilalahdentie 2-4, 02150 Espoo, FINLAND. Accordingly, Nokia Corporation is the real party in interest.

2. RELATED APPEALS AND INTERFERENCES

The appellant, assignee, and the legal representatives of both are unaware of any other appeal or interference which will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

3. STATUS OF CLAIMS

A. Claims canceled: 4

B. Claims withdrawn from consideration but not canceled: None

C. Claims pending: 1-3 and 5-11

D. Claims allowed: none

E. Claims rejected: 1-3 and 5-11

F. Claims appealed: 1-3 and 5-11

Appealed claims 1-3 and 5-11 as currently pending are attached as the Claims Appendix hereto. (Applicant notes that although the Advisory Action mailed October 7, 2009 indicates that the amendments presented in the Reply to the final Office Action, dated September 22, 2009, would *not* be entered, during a telephone conference held with the undersigned attorney on or about October 20, 2009, the Examiner indicated that an error had been made in the Advisory Action and that the amendments *would* be entered for purposes of an appeal.)

4. STATUS OF AMENDMENTS

A Reply under 37 C.F.R. §1.111 was filed on February 10, 2009; claim amendments were made. In response, the Examiner issued the final Office Action being appealed herein on May 22, 2009.

A Reply under 37 CFR §1.116 was filed on September 22, 2009; claim amendments were made. The submission of the Reply did not result in allowance by the Examiner.

5. SUMMARY OF THE CLAIMED SUBJECT MATTER

Claim 1: A method of operating a computing device, the method comprising, in response to a request from a user to carry out an operation using the device and for which the identity of the user is required to be authenticated, determining the time period since the identity of the user was last authenticated *[paragraphs [0033], [0034], Figure 1, steps 2-6, of the published application]*, and enabling the requested operation by determining the type of operation being requested by the user *[paragraphs [0033], [0034], Figure 1, steps 2-6, of the published application]* and enabling the operation only if the determined time period is valid for the type of operation requested by the user *[paragraph [0034] and steps 8-14 of Figure 1 of the published application].*

The claimed invention is predicated on the basis that a user must authenticate him/herself to a device, in order to carry out a particular operation, only if certain conditions apply. The conditions are the amount of time elapsed since the last authentication of the user occurred, and *the type of operation* being requested by the user.

The type of operation is significant, because if it is an operation that requires, for example, little or no security clearance (e.g., reading an email), the time between repeat authentications being required may be relatively long. However, if the type of operation requires substantial security clearance, for example, making purchases or other financial transactions, then the time between repeat authentications being required may be relatively short, or even zero, such that authentication is required every time.

The above is described in the U.S. patent publication corresponding to this application (US 2007/0289011) in paragraphs 0033 and 0034. A key feature of the invention is, therefore, the **type of operation** being requested. This feature is clearly recited in claim 1.

6. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Applicant requests the Board to review the following rejections:

1. Rejection of claims 1-4 and 8-11 under 35 U.S.C. §102(e) as being anticipated by U.S. Patent Application Publication No. 2004/0205176 to Ting et al.

2. Rejection of claims 5-7 under 35 U.S.C. §103(a) as being obvious over U.S. Patent Application Publication No. 2004/0205176 to Ting et al. in view of U.S. Patent Application Publication No. 2003/0074552 to Olkin et al.

7. ARGUMENT

1. Rejection of claims 1-4 and 8-11 under 35 U.S.C. §102(e) as being anticipated by U.S. Patent Application Publication No. 2004/0205176 to Ting et al.

In rejecting claim 1, the Office refers to paragraph [0009] of Ting as teaching the claimed element: "...enabling the requested operation by determining the type of operation being requested by the user and enabling the operation only if the determined time period is valid for the type of operation requested by the user." This assertion by the Office is incorrect, as nowhere in Ting is there any teaching or even suggestion of (a) determining the *type* of operation being requested by the user, or (b) enabling the operation only if the determined time period is valid for the *type of operation requested* by the user.

First, it is noted that the present application claims the determination of the type of operation requested by the user, and discloses in paragraph [0033] *examples* including an operation of a high-security type, such as a financial transaction, and an operation of a low-security type, such as reading an email. Nothing in Ting remotely teaches or suggests such a concept; Ting merely states in paragraph [0009] that access privileges may be revoked as a result of one or more trigger events, such as a broken communication connection, a changed password, the passage of time, or a sequence of events at the client or in the application. Nothing in this paragraph or anywhere else in Ting mentions anything about determining the type of operation being requested by the user as defined and claimed in the present application.

Second, the claimed invention enables the operation requested by the user only if the determined time period is valid for the *type of operation requested* by the user. This is disclosed in paragraph [0034] of the present application, and examples are given in paragraphs [0035] through [0050]. Nowhere in Ting is there any teaching or suggestion of this claimed feature; again, paragraph [0009] of Ting merely states that access privileges may be revoked as a result of one or more trigger events, such as a broken communication connection, a changed password, the passage of time, or a sequence of events at the client or in the application. Nowhere is there any discussion of controlling the enabling of a requested operation by only allowing the operation to proceed if an indentified time period elapsing is the appropriate time period for the *type of operation requested.* At best, Ting indicates that if a time period expires, OR if a communication connection has been broken, OR if a password has expired, OR if a password has been changed, OR if an unidentified sequence of events at the client, the application, or both has occurred, then a user can be made to re-authenticate their identity.

To summarize, Paragraph 9 in Ting describes trigger events stored in a user profile based on which the user is required to re-authenticate their identity. According to this paragraph, a user will be required to re-authenticate all the applications that are linked to his profile after the passage of time (or any other trigger event) set by the user. However, paragraph 9 fails to describe that the user will be required to re-authenticate if the passage time is valid for the type of operation requested by the user.

Paragraph 9 in Ting can be understood with help of the following example:

1. Passage of time is set to 1 hour
2. User signs a social networking site - Operation A
3. 10 minutes later user signs an email - Operation B. The user is not asked to reauthenticate as the passage of time has not expired.

4. 65 minutes later user signs another email - Operation B. The user is asked to reauthenticate as the passage of time has expired.
5. 20 minutes later user tries to make a financial operation - Operation C. The user is not asked to reauthenticate as the passage time has not expired.

It is apparent from the above example that the passage time in Ting is common for ***all operations*** and is <u>not</u> dependent on the ***type*** of operation. Hence, operations A, B, and C can be carried out as long as the passage time has not expired. Since the operation C described above is more sensitive/critical than operations A and B, its security can be compromised. The claimed invention solves this problem by authenticating a user based on the type of operation to be performed.

Each of the above elements are specifically claimed in the independent claim, and thus in all of the claims. Since these claimed elements are neither taught nor suggested by Ting, all of the claims are in allowable condition. For the reasons set forth above, the Board is respectfully requested to overrule the rejection of the claims under 35 U.S.C. §102.

2. Rejection of claims 5-7 under 35 U.S.C. §103(a) as being obvious over U.S. Patent Application Publication No. 2004/0205176 to Ting et al. in view of U.S. Patent Application Publication No. 2003/0074552 to Olkin et al.

<u>A *Prima Facie* Case of Obviousness Has Not Been Established</u>

KSR (*KSR International Co. v. Teleflex Inc.,* 127 S. Ct. 1727, 82 USPQ2d 1385 (2007) requires that the Office provide “some articulated reasoning with some rationale underpinning to support the legal conclusion of obviousness.” Further, the Office must “identify a reason that would have prompted a person of ordinary skill in the relevant field to combine the elements in the way the claimed new invention does,” In addition, the Office must make "explicit" this rationale of "the apparent reason to combine the known elements in the fashion claimed," including a detailed explanation of "the effects of demands known to the design community or present in the marketplace" and "the background knowledge possessed by a person having ordinary skill in the art."

Claims 5-7 are rejected under 35 U.S.C. §103 based on a proposed combination of Ting and Olkin. First, it is noted that claims 5-7 inherit the limitations of claim 1 and are thus patentable for the reasons set forth above regarding claim 1. Further, however, the addition of Olin does not teach or suggest the elements lacking in Ting as described above, and thus there is no teaching or suggestion to combine Ting and Olkin to achieve the invention of claims 5-7. Accordingly, the Board is respectfully requested to overrule the rejection of claims 5-7 under 35 U.S.C. §103.

8. CONCLUSION

For the foregoing reasons applicants respectfully request this Board to overrule the Examiner's rejections and allow claims 1-11.

Respectfully submitted:

January 20, 2010
Date

/Mark D. Simpson/
Mark D. Simpson
Reg. No. 32,942

SAUL EWING LLP
Centre Square West
1500 Market Street, 38th Floor
Philadelphia, PA 19102-2189
Telephone: 215 972 7880
Facsimile: 215 972 4169
Email: MSimpson@saul.com

CLAIMS APPENDIX

CLAIMS INVOLVED IN THIS APPEAL:

1. A method of operating a computing device, the method comprising, in response to a request from a user to carry out an operation using the device and for which the identity of the user is required to be authenticated, determining the time period since the identity of the user was last authenticated, and enabling the requested operation by determining the type of operation being requested by the user and enabling the operation only if the determined time period is valid for the type of operation requested by the user.

2. A method according to claim 1 wherein the identity of the user is authenticated using a pass phrase.

3. A method according to claim 1 wherein the identity of the user is authenticated using biometric information.

5. A method according to claim 1 wherein the requested operation is enabled if the determined time period is less than or equal to a time period set by the user.

6. A method according to claim 5 wherein the time period set for one type of operation is a multiple of a time period set for another type of operation.

7. A method according to claim 5 wherein the time period for a type of operation is arranged to expire upon completion of the immediately preceding operation of the same type.

8. A method according to claim 1 wherein categories of operations used to determine the purpose for a requested operation are set by the user.

9. A computing device arranged to operate in accordance with a method as claimed in claim 1.

10. A computing device according to claim 9 comprising a mobile phone.

11. Computer software arranged to cause a computing device to operate in accordance with a method as claimed in claim 1.

EVIDENCE APPENDIX

No additional evidence is presented.

RELATED PROCEEDINGS APPENDIX

No related proceedings are presented.